WHAT IS CLAIMED IS:

1. A method of authenticating an entity in a communication network system, comprising the steps of:

providing certificates of a first entity to be authenticated by a second entity on the basis of a certificate common to the first and second entities;

classifying the certificates of the first entity as a function of probability that a second entity includes a given certificate; and

in response to a certificate request by a second entity, submitting the classified certificate with highest probability to the second entity.

2. The method according to claim 1, wherein in case the certificate with highest probability is not present in the second entity, at least one further classified certificate is submitted to the second entity by decreasing likelihood, starting with the certificate with next-highest probability.

3. The method according to claim 1, wherein the classified certificates are evaluated on the basis of whether or not a submitted certificate is present in the second entity and classification of the certificates is updated on the basis of the evaluation result.

4. The method according to claim 1, wherein for classifying the certificates second entities are organized into groups, and within each group the certificates are ranked by their likelihood of being present in a second entity in the group.

5. The method according to claim 2, wherein for classifying the certificates second entities are organized into groups, and within each group the certificates are ranked by their likelihood of being present in a second entity in the group.

6. The method according claim 3, wherein for classifying the certificates second entities are organized into groups, and within each group the certificates are ranked by their likelihood of being present in a second entity in the group.

7. The method according to claim 4, wherein for each group a hit count is maintained with each certificate in the group, and if a certificate is submitted to a second entity belonging to given groups which certificate is present in the second entity, the hit count for each given group is increased, and on the basis of the hit counts the certificates are determined and ranked.

8. The method according to claim 4, wherein for each group a miss count is maintained with each certificate in the group, and if a certificate is submitted to a second entity belonging to given groups which certificate is not present in the second entity, the miss count for each given group is increased, and on the basis of the miss counts the certificates are determined and ranked.

9. The method according to claim 7, wherein for each group a miss count is maintained with each certificate in the group, and if a certificate is submitted to a second entity belonging to given groups which certificate is not present in the second entity, the miss count for each given group is increased, and on the basis of a hit probability derived from the hit counts and the miss counts the certificates are determined and ranked.

10. The method according to claim 4, wherein the second entities are arranged into groups based on at least one of the aspects of mobility, number of certificates present in the second entity, geographical information, prefix information and application information.

11. The method according to claim 7, wherein the second entities are arranged into groups based on at least one of the aspects of mobility, number of certificates present in the second entity, geographical information, prefix information and application information.

12. The method according to claim 8, wherein the second entities are arranged into groups based on at least one of the aspects of mobility, number of certificates present in the second entity, geographical information, prefix information and application information.

13. The method according to claim 9, wherein the second entities are arranged into groups based on at least one of the aspects of mobility, number of certificates present in the second entity, geographical information, prefix information and application information.

14. The method according to claim 4, wherein in response to a certificate request by a second entity the group to which the second entity belongs is determined according to a policy rule and certificates are submitted to the second entity based on the ranked certificates within the group.

15. The method according to claim 7, wherein in response to a certificate request by a second entity the group to which the second entity belongs is determined according to a policy rule and certificates are submitted to the second entity based on the ranked certificates within the group.

16. The method according to claim 8, wherein in response to a certificate request by a second entity the group to which the second entity belongs is determined according to a policy rule and certificates are submitted to the second entity based on the ranked certificates within the group.

17. The method according to claim 9, wherein in response to a certificate request by a second entity the group to which the second entity belongs is determined according to a policy rule and certificates are submitted to the second entity based on the ranked certificates within the group.

18. The method according to claim 10, wherein in response to a certificate request by a second entity the group to which the second entity belongs is determined according to a policy rule and certificates are submitted to the second entity based on the ranked certificates within the group.

19. An entity of a communication network system, comprising:

storage means for storing certificates of the entity to be authenticated by another entity of the communication network system based on a certificate common to both entities;

classification means for classifying the certificates of the entity as a function of probability that another entity includes a given certificate; and

in response to a certificate request by another entity, submission means for submitting the classified certificate with highest probability to the other entity.

20. The entity according to claim 19, wherein the entity is a serving network node of the communication network system.

21. The entity according to claim 19, wherein the other entity is a terminal of the communication network system.

22. A computer program product comprising software code portions for performing the steps, when run on a computer of:

providing certificates of a first entity to be authenticated by a second entity on the basis of a certificate common to the first and second entities;

classifying the certificates of the first entity as a function of probability that a second entity includes a given certificate; and

in response to a certificate request by a second entity, submitting the classified certificate with highest probability to the second entity.

23. The computer program product according to claim 22, wherein the product comprises a computer-readable medium on which the software code portions are stored.

24. The computer program product according to claim 22, wherein the product is directly loadable into the internal memory of the computer.